PRIME TIME

STRIDE ANALYSIS

Spoofing

- Potential Threat: The use of IP 10.0.0.176 for various attacks might involve spoofing, where the attacker disguises their identity. If this IP is not genuinely associated with the attacker, it could be an attempt to mislead the investigation.
- Affected Systems: Any system that relies on IP-based authentication could be at risk.

Tampering

- Potential Threat: Unauthorized changes made to system settings and user accounts, as observed in the Risk Analyst and CFO's systems, indicate tampering. This includes modifying Remote Desktop Protocol (RDP) settings and managing user accounts.
- Affected Systems: Risk Analyst 1 (10.0.0.74), CFO (10.0.0.206), and potentially other systems that were compromised and accessed by the attacker.

Repudiation

- Potential Threat: With the absence of strong audit trails and logging mechanisms, attackers could deny their malicious activities, such as unauthorized access or changes made to the systems.
- Affected Systems: All systems where unauthorized access was gained but not adequately logged, making it difficult to trace and prove the attacker's actions.

Information Disclosure

- Potential Threat: The successful brute force attacks, particularly on the Data Analytics Server (Server-BOB, 10.0.0.123), could lead to unauthorized access to sensitive information. Additionally, the creation of a malicious webpage on 10.0.0.175 could result in the exposure of sensitive data to unauthorized parties.
- Affected Systems: Data Analytics Server-BOB (10.0.0.123), Web App (10.0.0.175), and any system compromised that contained sensitive information.

Denial of Service (DoS)

- Potential Threat: While not directly mentioned, the attacker's activities, such as port scans and brute force attacks, could inadvertently lead to a denial of service by overwhelming the target systems, rendering them unresponsive.
- Affected Systems: Any system targeted by the brute force and port scanning activities, potentially leading to performance degradation or system crashes.

Elevation of Privilege

- Potential Threat: The attacker's attempts to modify system settings and introduce potentially malicious executables and DLLs suggest an attempt to elevate privileges within the compromised systems. This would allow the attacker to execute commands and access resources that are normally protected and restricted.

- Affected Systems: Risk Analyst 1 (10.0.0.74), where unauthorized changes were observed, and potentially any system where the attacker gained unauthorized access and could exploit vulnerabilities to elevate privileges.